



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/603,424	06/24/2003	Branislav N. Meandzija	15685P208	3310

45222 7590 03/06/2007  
ARRAYCOMM/BLAKELY  
12400 WILSHIRE BLVD  
SEVENTH FLOOR  
LOS ANGELES, CA 90025-1030

EXAMINER
----------

ARANI, TAGHI T

ART UNIT	PAPER NUMBER
----------	--------------

2131

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/06/2007	PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

**Office Action Summary**

Application No.

10/603,424

Applicant(s)

MEANDZIJA ET AL.

Examiner

Taghi T. Arani

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 16 January 2007.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-149 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-6, 10-24, 26-40, 42-48 is/are rejected.
- 7) ☐ Claim(s) 7-9, 25, 41 and 49 is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_.
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_.
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: \_\_\_\_\_.

### **DETAILED ACTION**

1. Claims 1-49 have been examined and are pending.

#### **Continued Examination Under 37 CFR 1.114**

2. A request for continued examination under 37 CFR 1.1 14, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.1 14, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.1 14. Applicant's submission filed on 1/16/2007 has been entered.

#### ***Response to Amendment***

3. Applicant's amendment filed 1/16/2007 necessitated the new ground(s) of rejection presented in this Office action. Applicant's arguments with respect to claims 1-48 have been fully considered but are moot in view of the new ground(s) of rejection.

#### ***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 1, 4-5, 10-13, 17, 20-21, 26-29, 33-37 and 42-45 are rejected under 35 U.S.C. 102(b) as being anticipated by Us patent 6,009,173 to Summer.

**As per claims 1, 17 and 33**, Summer teaches a method, a user terminal and a machine-readable medium performed by a user terminal of a wireless access network, the method comprising:

generating a shared secret to be provided to an access point of the wireless access network (Fig. 3, step 108, where sender-receiver session key is disclosed, see also col. 3, lines 32-34);

encrypting the shared secret with an access point public key (col. 3, lines 34-45, where the session key is encrypted using receiver's public key);

generating an authenticator string, the authenticator string demonstrating possession of a user terminal private key (col. 3, lines 19-32, i.e. a digital signature using sender's private key)

sending a message to the access point, the message including the encrypted shared secret, a user terminal certificate, and the authenticator string (col. 3, lines 33-52)

**As per claims 4, 20 and 36**, Summer teaches the method, the user terminal and the machine-readable medium of claims 1, 17 and 33, wherein generating the authenticator string comprises generating an authenticator message and signing the authenticator message with the user terminal private key (col. 3, lines 26-28).

**As per claims 5, 21 and 37**, Summer teaches the method, the user terminal and the machine-readable medium of claims 4, 20 and 36 respectively, wherein signing the authenticator message comprises:

generating a digest of the authenticator message (col. 3, lines 24-26); and

encrypting the authenticator message digest with the user terminal private key (col. 3, lines 26-28).

**As per claims 10 and 42**, Kaliski, Jr. teaches a method, a machine-readable medium performed by an access point of a wireless access network, comprising:

receiving a message from a user terminal of the wireless access network, the message containing a shared secret encrypted with an access point public key, a user terminal certificate, (col. 3, lines 53-65);

decrypting the shared secret using an access point private key (col. 3, lines 54-55);

authenticating the user terminal by checking the authenticator string using a user terminal public key included in the user terminal certificate to verify possession of the user terminal private key by the user terminal (col. 4, lines 1-24).

**As per claims 11 and 43**, Summer teaches the method and the machine-readable medium of claims 10 and 42 respectively, wherein the user terminal certificate is scrambled, and the access point unscrambles the user terminal certificate using the shared secret (col. 3, lines 56-59).

**As per claims 12 and 44**, Summer teaches the method and the machine-readable medium of claims 10 and 42 respectively, wherein checking the authenticator string comprises decrypting the authenticator string using the user public key (col. 4, lines 15-24 ).

**As per claims 13 and 45**, Summer teaches the method and machine-readable medium of claims 12 and 45 respectively, wherein checking the authenticator string further comprises generating an authenticator message, generating a digest of the authenticator message, and comparing the authenticator message digest with the decrypted authenticator string (col. 4, lines 19-24).

**Claims 26-29** correspond to an access point performing the steps recited method claims 10-12. Claims 26-29 are rejected for the same reason provided in the statement of rejections of claims 10-13 above.

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

**5. Claims 6, 22, and 38** are rejected under 35 U.S.C. 103(a) as being unpatentable over Summer as applied to claims 4, 20, and 36 and further in view of prior art of record, US patent 6,189,098 to Kaliski, Jr.

**As per claims 6, 22 and 38**, Summer teaches the method, the user terminal and the machine-readable medium of claims 4, 20 and 36 respectively. Summer does not teach but Kaliski, Jr. discloses wherein the authenticator message comprises a time parameter and at least part of the shared secret (col. 4, lines 39-51, i.e. (KSS||TS)PUBserver and (CERT-C)KSS). It would have been obvious to one of ordinary skill in the art at the time the

Art Unit: 2131

invention was made to employ the teachings of Kaliski, Jr. into the method and system of Summer to provide a time-varying message to provide safeguards against a third party impersonating the user terminal by simply replaying copies of the previous signatures intercepted or acquired (Kaliski, Jr., col. 1, lines 30-42).

**6. Claims 2-3, 14-16, 18-19, 30-32, 34-35 and 46-48** are rejected under 35 U.S.C. 103(a) as being unpatentable over Summer as applied to claims 1, 17 and 33 above, and further in view of prior art of record to Persson et al., US patent 6,754,824 (hereinafter "Person").

**As per claims 2, 18 and 34**, Summer teaches the method, the user terminal and the machine-readable medium of claims 1, 17 and 33 respectively, except wherein the user terminal certificate is scrambled, using a pseudo-random sequence generator initialized with a part of the shared secret, before being included in the message.

However, in an analogous art, Persson is directed to telecommunications systems and methods wherein the identity of the transmitting node is verified by modulating the CRC code utilizing a sequence known only to the participating parties. The modified CRC is generated by both the transmitting node and the receiving node initializing a LFSR register by a common key known only to the participating nodes (i.e. a pseudo-random sequence generated by a linear feedback shift register initialized with a part of the shared secret (Persson, col. 2, lines 5-23).

Therefore, it would have been obvious to one of ordinary skill at the time the invention was made to employ the teachings of Persson within the method and system of

Art Unit: 2131

Kaliski for combining Kaliski's certificate with a pseudo-random sequence generated by a linear feedback shift register initialized with a part of the shared secret in order to verify both the authenticity of the received certificate and the identity of transmitting node and to deter unauthorized party to replace the participating nodes if weak encryption or no encryption is switched on after authentication ( Persson, col. 1, lines 35-49).

**As per claims 3, 19 and 35**, once modified, Summer teaches. the method, the user terminal and the machine-readable medium of claims 2, 18 and 34 respectively, wherein the remainder of the shared secret comprises a master secret to be used for symmetric key cryptography between the user terminal and the access point (Kaliski, Jr., col. 4, lines 42-55, i.e. KSS is used for symmetric key cryptography, the remainder of KSS||TS).

**As per claims 14 and 46**, Summer teaches the method and the machine-readable medium of claims 13 and 45 respectively. Summer does not teach but Kaliski, Jr. discloses wherein the authenticator message comprises at least part of the shared secret (col. 4, lines 39-51, i.e. (KSS||TS)PUBserver). It would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teachings of Kaliski, Jr. into the method and system of Summer to include at least part of the shared secret in the authenticator message to provide safeguard s against a third party impersonating the user terminal by simply replaying copies of the previous signatures intercepted or acquired (Kaliski, Jr., col. 1, lines 30-42).

**As per claims 15 and 47**, Kaliski Jr. teaches the method and the machine-readable medium of claims 10 and 42 respectively, wherein the user terminal certificate is signed by a certificate authority trusted by the access point (col. 3, lines 63-67).

**As per claims 16 and 48**, Once modifies, Summer teaches the method and the machine-readable medium of claims 10 and 42, wherein the shared secret is to be used for symmetric key cryptography between the access point and the user terminal (Kaliski Jr. col. 4, lines 39-55, the shared secret session key KSS is used for symmetric key encryption between the client and the server).

**Claims 30-32** correspond to an access point performing the steps recited in method claims 14-16. Claims 30-32 are rejected for the same reason provided in the statement of rejections of claims 14-16 above above.

#### **Allowable Subject Matter**

7. **Claims 7-8, 9, 25 and 41 and 49** are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

#### **Conclusion**

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Taghi T. Arani whose telephone number is (571) 272-3787. The examiner can normally be reached on 8:00-5:30 Mon-Fri.

Art Unit: 2131

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Taghi T. Arani, Ph.D.  
Primary Examiner  
Art Unit 2131  
2/28/2007